

HİDROMEKANİK SURFACE TECHNOLOGIES	BİLGİ GÜVENLİĞİ POLİTİKASI	YÜRÜRLÜK TARİHİ : 21.02.2020 DOKÜMAN KODU : PLT-04 REV. NO/ TARİH: - SAYFA : 1/1
1. Giriş Bu Bilgi Güvenliği Politikası, organizasyonumuzun bilgi varlıklarının gizliliğini, bütünlüğünü ve erişilebilirliğini korumak amacıyla belirlenen temel ilke ve kuralları içerir. Amacımız, tüm bilgi varlıklarının güvenliğini sağlamak ve tüm çalışanları bilgilendirmek, bilinçlendirmek ve uygulamaları takip etmek yoluyla potansiyel riskleri en aza indirmektir. 2. Kapsam Bu politika, tüm çalışanlar, tedarikçiler, danışmanlar ve diğer ilgili taraflar için geçerlidir. Politikada yer alan hükümler, organizasyonun tüm dijital ve fiziksel bilgi varlıklarını kapsar. 3. Bilgi Güvenliği İlkeleri Gizlilik: Bilgilerin yalnızca yetkili kişiler tarafından erişilebilir olması sağlanmalıdır. Bütünlük: Bilgilerin doğru ve eksiksiz olması sağlanmalıdır. Erişilebilirlik: İlgili kişiler, gerekli bilgilere gerektiği zaman erişebilmelidir. İzlenebilirlik: Bilgi erişim ve değişiklikleri izlenebilir olmalıdır. 4. Sorumluluklar Çalışanlar: Tüm çalışanlar, bilgi güvenliği politikalarına uymakla yükümlüdür. Ayrıca, herhangi bir güvenlik ihlali veya zafiyet durumunda hemen yöneticilerine bildirimde bulunmalıdır. Yönetim: Üst yönetim, bilgi güvenliği politikasının uygulanmasını ve sürekli iyileştirilmesini sağlamakla sorumludur. BT Departmanı: Bilgi güvenliği önlemlerinin teknik uygulanmasını ve sistemlerin güvenliğini sağlamaktan sorumludur. 5. Bilgi Güvenliği Kontrolleri Erişim Kontrolleri: Tüm bilgilere erişim, yalnızca yetkilendirilmiş kişilere verilecek şekilde yönetilmelidir. Kullanıcı hesapları ve parola güvenliği en üst seviyede tutulmalıdır. Fiziksel Güvenlik: Sunucu odaları ve diğer kritik donanımlar, fiziksel güvenlik önlemleriyle korunmalıdır. Ağ Güvenliği: Ağ trafiği izlenmeli, güvenlik duvarları, virüs koruma yazılımları ve diğer güvenlik önlemleri kullanılmalıdır. Yedekleme ve Kurtarma: Veri kaybı durumunda hızlıca geri dönüş yapılabilmesi için düzenli yedeklemeler yapılmalı ve felaket kurtarma planları hazırlanmalıdır. 6. Eğitim ve Farkındalık Çalışanlar, bilgi güvenliği konusunda düzenli aralıklarla eğitimlere tabi tutulmalı ve bilinçlendirilmeli, her bir çalışanın kendi sorumluluğunda olan güvenlik önlemlerini uygulaması sağlanmalıdır. 7. Güvenlik İhlalleri ve Olay Yönetimi Güvenlik ihlali veya şüpheli bir olay durumunda, olaylar hızla tespit edilmeli ve rapor edilmelidir. Olay yönetimi süreci şeffaf bir şekilde yürütülmeli ve gerekli düzeltici önlemler alınmalıdır. 8. Politika İnceleme ve Güncelleme Bu politika, düzenli olarak gözden geçirilecek ve ihtiyaç duyulduğunda güncellenecektir. Politikanın güncel ve etkin olduğunun sağlanması için yıllık olarak gözden geçirilmesi tavsiye edilir. 9. Sonuç Bilgi güvenliği, organizasyonun sürdürülebilirliği ve itibarının korunması açısından kritik öneme sahiptir. Her çalışan, bu politikaya uymakla yükümlüdür ve güvenlik ihlali durumunda organizasyon tarafından gerekli disiplin cezaları uygulanabilir.		
HAZIRLAYAN GÖKHAN DOKUMACI	ONAYLAYAN Ahmet DOKUMACI	